FEDERAL PKI POLICY AUTHORITY

December 13, 2011 MEETING MINUTES

USPS Headquarters
475 L'Enfant Plaza, SW
Conference Room: 4841
Washington, DC
9:30 a.m. – 12:00 p.m. EST

09:30	**Welcome, Opening Remarks & Introductions**	**Deb Gallagher, Chair**
09:35	**Discuss / Vote on November 2011 FPKIPA Minutes**	**Matt King**
90:45	**FPKI Certificate Policy Working Group (CPWG) Report** **1. Review/Vote on DigiCert Cross-Certification at PIV-I** **2. Review/Update Status of CPWG Ongoing Initiatives** **a. Review/Update Status of RA Audit Change Proposal** **b. Review/Update Status of draft Criteria and Methodology** **c. Review/Update Status of FPKI CONOPS** **d. Review/Update Status of draft Incident Management Process Document** **e. Definition of CMS**	**Charles Froehlich**
10:15	**FPKI Management Authority (FPKI MA) Report**	**Darlene Gore**
10:45	**VA Status Update**	**Eric Jurasas**
11:00	**Other Agenda Items** o *ICAM Update—Deb Gallagher* o *If you cannot attend, please designate a proxy* o *Next FPKIPA meeting, January 10, 2011*	**Deb Gallagher**

11:15	**Holiday Social**	**All**
12:00	**Adjourn Meeting**	**Deb Gallagher**

A.

B. ATTENDANCE LIST

a. Voting Members

Organization	Name	T – Telephone P – In Person A – Absent
Department of Defense (DOD)	Mitchell, Debbie	T
Department of Energy (DOE)	Thomas, Michele	T
Department of Health & Human Services (HHS)	Slusher, Toby	T
Department of Homeland Security (DHS)	Miller, Tanyette	T
Department of Justice (DOJ)	Morrison, Scott	T
Department of State (State)	Frahm, Jarrod M.	P
Department of Treasury (Treasury)	Wood, Dan	A
Drug Enforcement Administration (DEA CSOS)	Briggs, Sherrod (Proxy for Chris Jewell)	A
Government Printing Office (GPO)	Hannan, John	T
General Services Administration (GSA)	Gallagher, Deb	P
National Aeronautics & Space Administration (NASA)	Wyatt, Terry	T
Nuclear Regulatory Commission (NRC)	Sulser, David	P
Social Security Administration (SSA)	Mitchell, Eric	T
United States Postal Service (USPS)	Stepongzi, Mark	P
United States Patent & Trademark Office (USPTO)	Lindsey, Dan	T
Veterans Administration (VA)	Jurasas, Eric	T

b. Observers

Organization	Name	T – Telephone P – In Person A – Absent
Cipher Solutions	Ahuja, Vijay	T
FPKI MA Technical Liaison (Contractor, Protiviti)	Brown, Wendy	P
DoS (Contractor, ManTech)	Froehlich, Charles	P
GSA, FPKI MAFPKIMA PM	Gore, Darlene	P
SSA (Contractor)	Hardy, Amy	P
USPTO (Contractor)	Jain, Amit	T
FPKIMA (Contractor, Protiviti)	Jarboe, Jeff	P
FPKIPA (Contractor, Protiviti)	King, Matt	P
FPKIMA (Contractor, Protiviti)	Kotraba, Matt	T
US Access (Contractor)	Lins, Andrew	T
FPKIMA (Contractor, Protiviti)	Louden, Chris	P
Veterans Administration (VA)	Miller, Jason	T
Entrust	Moore, Gary	P
Evalid8	Schminky, Jim	P
FPKIPA (Contractor, Protiviti)	Sonnier, Tiffany	P
CertiPath	Spencer, Judy	P

C. MEETING ACTIVITY

Welcome, Opening Remarks & Introductions, Deb Gallagher, Chair

The Federal Public Key Infrastructure Policy Authority (FPKIPA) met at the USPS Headquarters located at 475 L'Enfant Plaza, SW CR4841 Washington, DC. Ms. Deb Gallagher, Chair, called the meeting to order at 9:33 a.m. EST and those present, both in person and via teleconference, introduced themselves.

Discuss / Vote on November 8, 2011 FPKIPA Minutes, Matt King

There was a vote to approve the November 8, 2011 FPKIPA minutes. USPS motioned to approve; NRC seconded. The motion was approved unanimously.

Approval Vote for November 8, 2011 FPKIPA Minutes			
Voting members	**Vote (USPS Motion; NRC Second)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)			Absent
Department of Energy (DOE)	X		
Department of Health & Human Services (HHS)	X		
Department of Homeland Security (DHS)	X		
Department of Justice (DOJ)	X		
Department of State (State)	X		
Department of the Treasury (Treasury)			Absent
Drug Enforcement Administration (DEA CSOS)			Absent
Government Printing Office (GPO)	X		
General Services Administration (GSA)	X		
National Aeronautics & Space Administration (NASA)	X		
Nuclear Regulatory Commission (NRC)	X		
Social Security Administration (SSA)	X		
United States Postal Service (USPS)	X		
United States Patent & Trademark Office (USPTO)	X		
Veterans Administration (VA)	X		

FPKI Certificate Policy Working Group (CPWG) Report, Charles Froehlich

1. Review/Vote on DigiCert Cross-Certification at PIV-I

There was a vote to approve DigiCert at PIV-I. DigiCert was previously approved for FBCA cross certification, but there was a delay in testing their PIV-I card and CMS. In addition, DigiCert also wants to add the Device Certificate policy OIDs. Testing is now complete. GSA motioned to approve; USPS seconded. The motion was approved unanimously.

Approval Vote for DigiCert Cross-certification at PIV-I			
Voting members	**Vote (GSA Motion; USPS Second)**		
	Yes	**No**	**Abstain or Absent**
Department of Defense (DOD)	X		
Department of Energy (DOE)	X		
Department of Health & Human Services (HHS)	X		
Department of Homeland Security (DHS)	X		
Department of Justice (DOJ)	X		
Department of State (State)	X		
Department of the Treasury (Treasury)			Absent
Drug Enforcement Administration (DEA CSOS)			Absent
Government Printing Office (GPO)	X		
General Services Administration (GSA)	X		
National Aeronautics & Space Administration (NASA)	X		
Nuclear Regulatory Commission (NRC)	X		
Social Security Administration (SSA)	X		
United States Postal Service (USPS)	X		
United States Patent & Trademark Office (USPTO)	X		
Veterans Administration (VA)	X		

2. Review/Update Status of CPWG Ongoing Initiatives

a. Review/Update Status of RA Audit Change Proposal

Discussions were held about Registration Authority (RA) and CMS audit requirements. This issue is related to the VA incident since there were questions raised about which organization has responsibility for auditing the RA function when an agency uses a Shared Service Provider (SSP), but performs some of the RA functions within the agency. The CPWG agreed to develop change proposals for Common and Bridge to clarify the audit requirements. In addition, the CPWG agreed to add statements in the FBCA and Common certificate policies regarding the purpose of a compliance audit.

Some CPWG members wanted to know why the change proposal was needed, and had concerns about providing full-audit reports to the FPKIPA. It was clarified that under the FBCA Certificate Policy, the audit reports are submitted to the Certification Authority (CA) owner, and that the CA owner submits Compliance Audit Letters to the FPKIPA in accordance with the "audit cookbook."

For SSPs under Common, CA Owners have a choice: (1) they can audit all functionality of their infrastructure, or (2) delegate audit responsibility to organizations that operate components of the PKI on the CA owner's behalf. The SSP customer that performs their own audit of the RA/ CMS functions must submit an audit report to the CA Owner.

Discussions in the CPWG also included whether the requirement for all independently-managed portions of a PKI to be audited is already implicitly required by policy, and therefore this change proposal is unnecessary. Auditing hundreds or thousands of RAs each year is nearly impossible. This change proposal should help an SSP that does not have authority to insist that its federal customers perform the annual audit (i.e., make sure that the SSP can pass at least a portion of the annual audit responsibility on to their customer). This change proposal clarifies that if functions have been farmed out to other organizations, the CA owner is still responsible for ensuring its completion. Change proposals for the FBCA and Common Certificate Policies were discussed. The CPWG essentially agreed on language for the FBCA Change Proposal, and sent the change proposal to the CPWG and FPKIPA mail lists with an explanation of the purpose of the RA/CMS Audit Requirements, and a request for participation in the December 20, 2011 CPWG meeting.

Ms. Judy Spencer asked if the requirements would still allow a sampling of RAs to be audited, and Mr. David Sulser clarified a sampling was still permitted.

The current language in the Common Policy Certificate Policy says the Audit Report is sent to the FPKIPA, while the FBCA Certificate Policy only requires the Audit Letter. Ms. Spencer suggested that Mr. John Cornell be consulted to determine if the full audit report was required or just an audit letter. Ms. Gallagher stated that we don't want a policy that requires submission of a document that could expose vulnerabilities. Mr. Jim Schminky stated that Treasury has always submitted an audit letter, even for their SSP, but it was agreed that the full audit report could be requested if necessary.

ACTION:

1. Mr. Matt King will consult Mr. John Cornell and Mr. Tim Polk to determine if the intent of the Common Policy audit requirements is to require an Audit Letter or a full Audit Report.

b. Review/Update Status of draft Criteria and Methodology

The CPWG has completed the review, and updated of the FBCA Cross Certification Criteria and Methodology document, which was circulated for FPKIPA review on December 4, 2011.Some of the more significant changes and updates included:

1. Allows Legacy Federal PKIs to cross-certify directly with FCPCA; but since they are mapped to the FBCA, Crits and Methods still applies in terms of maintaining compliance.
2. Added additional requirements for PIV-I issuers in terms of PIV-I card testing and PIV-I Certificate Profiles; PIV-I Card testing is considered part of Technical Testing, which used to be called Technical Interoperability Testing.
3. Includes the “New way of Mapping” for policy analysis.
4. Changed to allow optional Directory support, but requires Applicants and Affiliate to provide information about all Repositories used to support URLs in issued certificates.
5. Added that an Applicant’s third-party auditor should not represent the Applicant during the mapping process (can still be present).
6. Clarified the change proposal process to include a delta mapping matrix, and required response from each Affiliate before the FPKIPA vote.
7. Clarified compliance monitoring by requiring annual audit report to include documentation that the Affiliate is in compliance with all FBCA change proposals whose implementation date has passed since the last audit.
8. Added that Audit reports include evidence of compliance for all independently-operated components of the Affiliate PKI.

No vote by the FPKIPA is required. However, if there are any comments, they should be identified at this time for CPWG review.

Ms. Spencer mentioned that CertiPath requires members to send a delta certificate policy, and vice versa – CertiPath also only issues one year certificates.

Ms. Darlene Gore asked if there is a document that lists the current status of FPKI documents under review. Mr. King stated that
such a list exists and would be revised for distribution.

In addition, Dave Sulser suggested a tickler list/shared calendar would be a good way to keep the FPKIPA community informed.

ACTION:

1. Mr. King will evolve the document tracking table to provide detailed status for the FPKI Community (NIST documents that are in the review process should also be included).

c. Review/Update Status of FPKI CONOPS

The CPWG has continued work on the FPKI CONOPS—the initial version has been reviewed and comments incorporated. On December 20, 2011, the CPWG will discuss (1) concerns regarding how comments were addressed, and (2) suggestions for improving process flows.

d. Review/Update Status of draft Incident Management Process Document

The Incident Management Process document has been submitted to the CPWG for initial review and comment. The Incident Management Tiger Team will review and address the comments. Unresolved comments will be discussed at the January 24th CPWG meeting for review. The Four Bridges Forum (4BF) suggested leveraging the incident management process for the wider 4BF community.

It was noted that revocation thresholds will not be addressed in the current draft (since it was just raised in the 4BF) but will be evaluated in the future. In addition, no use cases will be included in the current draft, but will be added in the future to show how these incidents would have been handled if the process had been in place.

It was also suggested that the incident process should consider including a comparison of how the incident actually was handled vs. how it might have been handled under incident management process to identify best practices and lessons learned.

e. Definition of CMS

Discussion of the CMS definition was held during the past two meetings. The term could mean: (1) Certificate Management System; (2) Cryptographic Module; or (3) Card Management System. State and local organizations have read the PIV-I policy requirements and believe they require additional auditing. These organizations view the requirements as a barrier to entry into the FPKI because it’s another $1M per year for required audits besides just the Card Management System.

The FBCA Certificate Policy was reviewed, and requirements related to CMS were identified. The CPWG agreed that the CMS requirements in the FBCA were appropriate for PIV-I and that Medium Level of Assurance audit requirements do apply to PIV-I and associated CMSs. Therefore, if a state/local wants to issue PIV-I cards, they must have a CMS and comply with the audit requirements.

The CPWG felt that requirements are clear, but the CPWG welcomes the state/local organizations that identified the issue to present at a future CPWG, and to ask for further direction.

FPKI Management Authority (FPKIMA) Report, Darlene Gore

Ms. Gore and Ms. Wendy Brown presented the FPKIMA report. A certificate was issued to the ORC NFI PKI. In addition, certificates were issued to VeriSign to remove name constraints, which will allow them to issue to federal customers.

The number of requests of the FPKI Trust Infrastructure has surpassed 1 Billion. The FPKIMA will invest in software to analyze where traffic is coming from, but expects that most of the traffic in increase is due to OMB M-11-11 memo requirements. An update of FPKIMA Technical Working Group (TWG) activities was also presented. Microsoft has not responded to the request for an extension on the requirement to support a Timestamp Authority that was submitted on behalf of the FPKI. While there is no update on the Path Validation issue previously discussed, a new path validation issue will be discussed at the TWG meeting on December 20, 2011. Work continues on the Trust Stores Guidance document, which will also be discussed at the next TWG meeting.

VA Status Update. Eric Jurasas

Mr. Eric Jurasas and Mr. Jason Miller from Veteran's Affairs (VA) were asked to provide an update on progress of the mitigation steps being taken by the VA in response to compliance violations the VAOIG had listed in their recent report. There were no changes, and VA is working out the contractual details of bringing in an independent auditor to perform an Independent Validation and Verification (IV&V) or audit. In the meantime, VA is continuing to progress with their mitigation plan. The VA plan was briefed at the November 2011 FPKIPA meeting, and distributed on November 21, 2011.

Other Agenda Items, Deb Gallagher

1. ICAM Update

Ms. Gallagher provided updates of various ICAM efforts. Part 2 of the FICAM roadmap and implementation Guidance document has been issued and posted on IDManagement.gov. As a result, chapters 6-12 (implementation and best practices) are now published. It was noted that the Wiki feature has not been implemented.

Ms. Gallagher noted that all ICAM Working Groups (WGs) are being reviewed by the ICAMSC, and there should be a briefing about this soon. Originally, some of the WGs were focused on coming up with information for the roadmap (which is nearing completion) and ICAM work is increasing, so ICAMSC is looking at ways to reorganize the working groups and leverage the momentum and expertise to provide the necessary support to ICAM initiatives as they evolve beyond roadmap development.

The E-Signature Guidance document is going through the LRM (legal review) and it will be posted soon to IDManagement.gov. Minor changes were made by Justice and DoD lawyers.

Verizon is a new Identity Provider (IdP) under TFET, approved at assurance levels 1-3. Ms Spencer commented that sometimes people don't realize that the FPKIPA and

TFET are interlocking bodies for approving level 3 and 4 credentials, so it might be beneficial to clarify that FPKI and TFET are working together.

NIST Special Publication 800-63-1 was published, so there may be impacts of which members should be aware.

An ICAM Day will be held at the end of February 2012. It may be open to a wider audience than last time.

There are now two development sites for using assurance level 1 - 3 on IDManagement.gov, and we are hoping to stand it up in January 2012. This aligns with cloud requirements, so we need to coordinate to ensure security boundaries are set properly.

2. If you cannot attend, please designate a proxy

The next ICAMSC Meeting is next January 25, 2012.

The next FPKIPA Meeting is January 10, 2012.

Next CPWG meeting is December 20, 2011.

<u>Adjourn Meeting</u>

Ms. Gallagher adjourned the business portion of the FPKIPA meeting at 11:05 a.m. EST, so the holiday party could begin.

FPKIPA Action Items

No.	Action Statement	POC	Start Date	Target Date	Status
433	Matt King will place a deadline for C4CA responses for the first August CPWG for all agencies to provide their position on the necessity of the C4CA	Matt King	July 12, 2011	August 8 2011	Closed
434	Ms. Brown will send the MA report to the PA after changing the TWG date.	Wendy Brown	July 12, 2011	July 19, 2011	Closed
435	Ms Cheryl Jenkins will arrange an ad hoc meeting with Microsoft to address the CAPI path validation issues prior to Sept 15, 2011	Cheryl Jenkins	July 12, 2011	September 15, 2011	Closed
436	Ms. Gallagher will send an email with the request for a statement of need for removing the non-revocable certificates to the voting PA members .	Deb Gallagher	July 12, 2011	August 9, 2011	Closed
437	Mr. Matt King will send the EGTS briefing to the group	Matt King	July 12, 2011	August 9, 2011	Closed
438	Ms Gallagher will publish the Digital Signature Guidance once a final review is complete; will be published on the web as well.	Deb Gallagher	July 12, 2011	September 13, 2011	Open

No.	Action Statement	POC	Start Date	Target Date	Status
439	Ms. Wendy Brown and Mr. Matt King work to establish a fed-only email list.	Matt King / Wendy Brown	August 9, 2011	December 13, 2011	closed
442	Mr. King will send ORC PIV-I testing documentation and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
443	Mr. King will send DigiCert audit letter and E-vote to the FPKIPA mail list	Matt King	August 9, 2011	September 13, 2011	Closed
446	The Timestamp Server White Paper will be added to the CPWG and FPKIPA agendas.	FPKIMA	August 9, 2011	September 13, 2011	Closed
449	All FPKIPA members shall submit their nomination for a new FPKIPA Chair to Ms. Gallagher and Mr. King by October 31, 2011	All Voting Members	September 13, 2011	October 31, 2011	Closed
450	Ms. Mitchell will provide DoD Lessons Learned from the LDAP transition by Oct 6, 2011.	Debbie Mitchell	September 13, 2011	October 6, 2011	Closed
451	At the 25 October meeting, the CPWG will add language to the FPKIPA Charter – Option B indicating that the CIO Council will appoint the FPKIPA Chair from a list of nominees put forward by the FPKIPA membership	Matt King	October 18, 2011	October 25, 2011	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
452	At the 25 October meeting, the CPWG will discuss revising the FBCA Device Change Proposal to address Mr. Cooper's concerns that language in the FBCA change proposal was unnecessary	Matt King	October 18, 2011	October 25, 2011	Closed
453	Mr. Matt King to obtain Ms. Gallagher's signature on Charter and post to idmanagemnt.gov	Matt King	Nov 8, 2011	Dec 13, 2011	Open
454	Ms. Gallagher and Mr. King to find out what's needed to participate in CAB Forum.	Matt King, Deb Gallagher	Nov 8, 2011	Dec 13, 2011	Open
455	Mr. Hancock of VA will send the VA status briefing presented in the 8 November FPKIPA meeting to Matt King for distribution and report back with a VA mitigation plan at the next FPKIPA meeting.	Matt King, John Hancock (Va)	Nov 8, 2011	Dec 13, 2011	Closed
456	Mr. King to distribute the VA briefing summarizing actions taken as of November 8, 2011 once the briefing is received from VA.	Matt King	Nov 8, 2011	Dec 13, 2011	Closed
457	Mr. Matt King will consult Mr. John Cornell and Mr. Tim Polk to determine if the intent of the Common Policy audit requirements is to require an Audit Letter or a full Audit Report.	Matt King	Dec 13, 2011	Jan 10, 2012	Closed

No.	Action Statement	POC	Start Date	Target Date	Status
458	Mr. Matt King will evolve the document tracking table to provide detailed status for the FPKI Community (NIST documents that are in the review process should also be included).	Matt King	Dec 13, 2011	Mar 30, 2012	Open